AMENDMENTS TO THE SPECIFICATION:

Please amend the heading beginning at page 1, line 3, as follows:

~~Field of the Invention~~Introduction

Please amend the paragraph beginning at page 1, line 5, as follows:

~~The present invention relates to~~ This case describes secure traffic redirection in a mobile communication system and in particular to a method and apparatus for enabling a mobile node to securely perform transactions, relating to traffic redirection, with a home network.

Please amend the heading beginning at page 1, line 9, as follows:

Background ~~to the Invention~~

Please amend the heading beginning at page 2, line 23, as follows:

Summary ~~of the Invention~~

Please amend the paragraph beginning at page 2, line 25, as follows:

It is an object ~~of the present invention~~ to make use of existing security mechanisms to bootstrap whatever security may be required by the mobility services and mechanisms.

Please amend the paragraph beginning at page 2, line 28, as follows:

According to a first aspect ~~of the present invention~~ there is provided a method of securely ~~initialising~~ initializing subscriber and security data in a mobile routing system when the subscribers are also subscribers of a radio communication network, the method comprising:

Please amend the paragraph beginning at page 3, line 16, as follows:

In a first example embodiment ~~of the invention~~ the mobile routing system is a MobileIP based system, in which case the mobility server is a Home Agent. In an alternative example embodiment ~~of the invention~~ the mobile routing system is a HIP based system and the mobility server is a Forwarding Agent.

Please amend the paragraph beginning at page 3, line 24, as follows:

According to a second aspect ~~of the invention~~ there is provided a method of operating a mobile node for use in a ~~[[ ]]~~mobile radio communication system, the method comprising:

Please amend the paragraph beginning at page 3, line 31, as follows:

According to a third aspect ~~of the present invention~~ there is provided a method of operating a mobility server of a mobile routing system, the method comprising:

Please amend the paragraph beginning at page 4, line 7, as follows:

According to a fourth aspect ~~of the present invention~~ there is provided a method of operating an authentication server of a mobile radio communication network, the method comprising;

Please amend the heading beginning at page 4, line 20, as follows:

Detailed Description~~ of Certain Embodiments~~

Please amend the paragraph beginning at page 4, line 22, as follows:

Procedures have been defined and specified for allowing a mobile node to be securely authenticated by a home network in a cellular communication system. For example, the 3GPP authentication procedure known as Authentication and Key Agreement (AKA) makes use of a secret key stored in the Subscriber Identity Module (SIM) card of a cellular device and in the HSS node of the subscriber's home network to authenticate the cellular device (or rather the SIM card) at the network level. In the case of a roaming cellular device, the AKA procedure is performed via the visited network, with the home network informing the visited network of the authentication decision. ~~Whilst~~ While alternatives to AKA exist and fall within the scope of ~~this invention~~the claims, the present discussion will be restricted to AKA by way of non-limiting example.

Please amend the paragraph beginning at page 7, line 14, as follows:

Step 11. The mobile node 1 stores the received information. Note that this information has to be handled in a special way if a separation exists between a device and the user's credentials such as is common in phones and SIM cards inserted into them. Leaving the information in the device for use by any user (SIM card) would allow the use of this information by other users. This risk can be mitigated by storing the received information in the SIM, or storing it in the device in a manner which ~~isn't~~ is not accessible after another SIM [[ ]]has been inserted.

Please amend the paragraph beginning at page 8, line 1, as follows:

There ~~exists~~ may be proposals that make use of cell phone authentication in other contexts (e.g. RFC 3310)~~, so the reuse of SIM authentication itself is not new~~. ~~Here, however,~~ But here the authentication procedure is used in a specific way for a specific application, with additional procedures for collecting at the mobility server (i.e. the Home or Forwarding Agent) information from the subscriber database or databases.

Please amend the paragraph beginning at page 8, line 8, as follows:

There ~~exists~~ may be proposals that make use of cell phone authentication even in the context of, e.g., Mobile Ipv6. However, ~~these~~ such proposals would use such authentication each time a transaction is carried out between the mobile node and the mobility server, and lack a mechanism to decide the IP addresses and FQDNs.

Please amend the paragraph beginning at page 8, line 13, as follows:

There also ~~exists~~ may be proposals to use cell phone and other legacy authentication mechanisms to generate so called subscriber certificates in a general fashion, suitable for any application. However, the ~~solutions~~ technology described here ~~avoid~~ avoids this step, and avoid the use of any PKI other than the resulting DNS system as a "weak" form of PKI. In addition, the ~~presented solutions are clearly able to~~ technology here can make the necessary authorisation decisions regarding FQDNs and IP addresses, unlike the existing proposals.

Please amend the paragraph beginning at page 8, line 29, as follows:

~~Embodiments of the invention should~~ Example embodiments enable easy deployment of mobility services in heterogeneous networks.

Please amend the paragraph beginning at page 8, line 32, as follows:

The above discussion has considered the scenario where the access network is the same when both the initial, network level authentication procedure and the re-run procedure are carried out. A question to be addressed is what happens if a mobile node moves between different access networks which might use different authentication procedures. Consider for example the scenario in which a mobile node roams between a UMTS access network and a WLAN access network. ~~Whilst~~ While the UMTS network will use AKA to authenticate subscribers at the network level, the WLAN network might use some other procedure at this level. The ~~present invention~~ technology described encompasses the possibility that, after the WLAN network level access procedure has been carried out, the AKA procedure is reused to authorise the subscriber in respect of the mobility service.

Please amend the paragraph beginning at page 9, line 10, as follows:

It will be appreciated by the person of skill in the art that various modifications may be made to the embodiments described above without departing from the scope of the ~~present invention~~claims.